UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/553,790	10/19/2005	Francesco Pessolano	NL03 0397 US1	4003

65913 7590 04/28/2011
NXP, B.V.
NXP INTELLECTUAL PROPERTY & LICENSING
M/S41-SJ
1109 MCKAY DRIVE
SAN JOSE, CA 95131

EXAMINER	
KING, JOHN B	
ART UNIT	**PAPER NUMBER**
2435	
NOTIFICATION DATE	**DELIVERY MODE**
04/28/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ip.department.us@nxp.com

Office Action Summary	**Application No.** 10/553,790	**Applicant(s)** PESSOLANO, FRANCESCO
	Examiner John B. King	**Art Unit** 2435

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 February 2011*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8,13 and 14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8,13 and 14* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-8 and 13-14 are pending in this application.

2. Claims 9-11 and 12 have been canceled.

Response to Arguments

3. Applicant's arguments filed February 22, 2011 have been considered but they are not persuasive. In the remarks applicant argues:

I) The examiner's use of MPEP 2144.04 (V)(B) is misplaced as this "would make the circuits more vulnerable to the attacks described in Thueringer".

II) Thueringer only teaches "generating cloaking currents for each logic circuit separately".

In response to applicant's arguments:

I) The examiner respectfully disagrees. Thuringer does not teach away from this concept. Thuringer merely teaches that it is preferable to have the load circuit and the data processing device combined into a single circuit for a specific reason. MPEP 2144.04(V)(B) states that making integral things separable is “merely a matter of obvious engineering choice”. Therefore, it would have been an obvious design choice to break the load circuit of Thuringer into multiple other components i.e. a monitoring component and a current drawing component. This would make the interchangeability of the parts easier. For example, when only one component is used and the monitoring aspect breaks, the entire load circuit will have to be changed. However, if two components are used and the monitoring aspect breaks only the monitoring circuit will have to be changed.

II) The examiner respectfully disagrees. Thuringer, col. 1 lines 25-65, teaches the load circuit being controlled by the power consumed by the data processing device. The data processing device is a circuit arrangement (has multiple circuits) and the total power consumption used by the data processing device is a sum of the power used by all of these separate circuit components. Thüringer also teaches that the load circuit produces a current to be complementary to the rest of the circuit. Therefore, the load current (cloaking current) is added to the total power consumption of the data processing device to prevent third parties from determining the secret information by measuring the power consumed by the data processing device. Therefore, the load current is generated based on the total power consumption of the data processing device, which is the summation of the power consumed by each of the circuit components of the data processing device.

Examiner Notes

4. Examiner cites particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that, in preparing responses, the applicant fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. **Claim 1** is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

7. Claim 1 recites “an activity monitor circuit, coupled to receive pairs of processing signals” and later “the activity monitor circuit is coupled to receive a pair of processing signals”. It is unclear if these pairs of processing signals are the same or different.

8. Claim 1 recites “a combined activity signal” on line 12 and later “a combined activity signal" on line 24. It is unclear is these combined activity signals are intended to be the same signal or a different signal.

9. Claim 1 recites “a sum of power supply currents” on lines 12-13 and later on line 25. It is unclear if these sums of power supply currents are intended to be the same or different.

10. The examiner has cited particular examples of 35 U.S.C. 112 rejections above. It is respectfully requested that, in preparing responses, the applicant check the claims for further 35 U.S.C. 112 rejections in the event that it was inadvertently missed by the examiner. The following prior art rejections are based upon the examiner’s best interpretation of the claims.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. **Claims 1, 5, 7, and 13** are rejected under 35 U.S.C. 103(a) as being unpatentable over Thüringer et al. (US 6498404 B1) hereinafter referred to as Thüringer.

As per claims 1 and 7, Thüringer discloses an electronic circuit device for executing operations dependent on secret information, the electronic circuit device, comprising: power supply connections **(Thuringer, col. 1 lines 28-32 and col. 2 lines 28-30, teaches the use of power supplies.)**;

a processing unit **[data processing device]** comprising a plurality of processing circuits for use in execution of respective parts of the operations dependent on the secret information **(Thuringer, col. 1 lines 5-52, teaches a circuit arrangement for performing security-relevant operations where the security-relevant operations involve processing secret information as indicated in col. 2 lines 62-67 through col. 3 lines 1-6.)**, the processing circuits being fed from the power supply connections **(Thuringer, col. 1 lines 34-38, teaches monitoring the power consumption of the data processing device.)**;

an activity monitor circuit coupled to receive pairs of processing signals, each of the pairs of processing signals including an input signal **[power connection]** and an output signal **[power consumption of data processing device]** of one of the processing circuits **(Thuringer, Figure 2, teaches a load circuit that takes in a pair of signals and then outputs a pair of signals after processing. Thuringer, col. 1 line 45-col. 2 line 9, teaches that the load circuit monitors the power consumption of the data processing device. The input signal for the load circuit is the power connections i.e. Vcc (otherwise the circuit will not be functional) and also the output power consumption of the data processing device.)**,

the activity monitor circuit being arranged to derive activity information derived from each pair of processing signals, the activity information indicative of whether each of the processing circuits generates a logic level transition **(Thuringer, col. 2 lines 47-60, teaches the circuit determining if the incoming logic signals are high or low. Thuringer, col. 1 lines 52-60, teaches monitoring the logic states of the power consumption.)**,

and to derive from the activity information a combined activity signal indicative of a sum of power supply currents that will be consumed by the processing circuits dependent on the processing signals **(Thuringer, col. 1 lines 46-65, teaches the load circuit being controlled by what happens in the data processing device.**

Thüringer, col. 1 lines 46-52, teaches that the load circuit produces a current to be complementary to the rest of the circuit. Therefore, the load current is being added to the current that the data processing device is drawing to prevent third parties from determining the secret information by measuring the power consumed by the data processing device. The data processing device is a circuit arrangement (has multiple circuits) and the total power consumption used by the data processing device is a sum of the power used by all of the separate circuit components.);

a current drawing circuit connected to the power supply connections and controlled by the activity monitor circuit to draw a cloaking current controlled by the combined activity signal **(Thuringer, col. 1 lines 28-38, teaches having a load circuit connected to the power supply to mask the measurable power consumption of the data processing device.)**,

so that power supply current variations dependent on the secret information are cloaked in a combination of the cloaking current and current drawn by the processing circuits **(Thuringer, col. 1 lines 46-52, teaches that the load circuit draws additional current to cloak (or mask) the power consumed by the data processing device to prevent attackers from retrieving the secret key as in col. 1 lines 12-23.)**;

characterized in that the activity monitor circuit is coupled to receive a pair of processing signals for each of the pairs of processing circuits, coming into and out of the processing circuit respectively **(Thuringer, Figure 2, teaches a load circuit that takes in a pair of signals and then outputs a pair of signals after processing.**

Thuringer, col. 1 line 45-col. 2 line 9, teaches that the load circuit monitors the power consumption of the data processing device. The input signal for the load circuit is the power connections i.e. Vcc (otherwise the circuit will not be functional) and also the output power consumption of the data processing device.),

the activity monitor circuit being configured to derive the activity information from each pair of processing signals and to derive from the activity information for said processing circuits a combined activity signal dependent on the processing signals indicative of a sum of power supply currents that will be consumed by said processing circuits in combination **(Thuringer, col. 2 lines 47-60, teaches the circuit determining if the incoming logic signals are high or low. Thuringer, col. 1 lines 52-60, teaches monitoring the logic states of the power consumption. Thüringer, col. 1 lines 46-52, teaches having a data processing device, which is a circuit arrangement i.e. has multiple circuits. The total power consumption of the data processing device is the sum of the power used by all of the separate circuit components. The load circuit is then added to the total power consumption of the data processing device to prevent third parties from determining the secret information by measuring the power consumed by the data processing device.)**

the activity monitor circuit being coupled to the current drawing circuit to control generation of the cloaking current under control of the combined activity signal **(Thuringer, col. 1 lines 46-65, teaches the load circuit being controlled by what**

happens in the data processing device. The load circuit produces a current to mask/cloak the readable power consumption.)

However, Thuringer teaches having a single load circuit instead of having an activity monitor circuit and a current drawing circuit. The load circuit performs the same task as the activity monitor circuit and the current drawing circuit.

It would have been obvious to one of ordinary skill in the art to modify the invention of Thuringer by dividing the load circuit into multiple other circuits such as a monitoring component and a current drawing component. Thuringer teaches having a single load circuit that performs both the monitoring and the current drawing aspects of the Instant Application, and MPEP 2144.04(V)(B) states that making integral things separable is “merely a matter of obvious engineering choice”. Therefore, it would have been obvious to break the load circuit of Thuringer into multiple other components i.e. a monitoring component and a current drawing component. This would make the interchangeability of the parts easier. For example, when only one component is used and the monitoring aspect breaks, the entire load circuit will have to be changed. However, if two components are used and the monitoring aspect breaks only the monitoring circuit will have to be changed.

As per claim 5, Thüringer discloses an electronic circuit device according to claim 1 **[See rejection to claim 1 above]**, having a trigger input coupled to the current drawing circuit **(Thüringer, Figure 3 and col. 3 lines 17-23, teaches having a voltage signal, V, connected to the switching transistors to control the load resistors.)**,

arranged to enable drawing of the cloaking current only upon receiving a trigger signal that triggers or accompanies execution of a secret information dependent process in the electronic circuit device **(Thüringer, Figure 3 and col. 3 lines 17-23, teaches having transistors connected to the load circuit resistors. Therefore, the load current will only be drawn when the transistors are switched on, when the voltage V signal is high. This is performed to control the value of the cloaking current so that the measurable power consumption is not always constant.)**

As per claim 13, Thuringer discloses the electronic circuit device of claim 1 **[See rejection to claim 1 above]**,

wherein the current drawing circuit is a digital to analog converter that is configured to convert a digitally coded value into an analog power supply current that is equal to the cloaking current **(Thuringer, col. 1 line 45-col. 2 line 9, teaches outputting the masking or cloaking current as an analog signal. If the current reference (constant value) is entered/stored/generated as a digital value, it would have been obvious to use a digital to analog converter to convert the value to output the cloaking current as an analog value as taught by Thuringer.)**

13. **Claims 2-4** are rejected under 35 U.S.C. 103(a) as being unpatentable over Thüringer in view of NPL by Patterson et al. (Computer Architecture : A Quantitative Approach) pages 134-135 published in 1995, hereinafter referred to as Patterson.

As per claim 2, Thüringer discloses an electronic circuit device according to claim 1 **[See rejection to claim 1 above]**,

wherein the processing unit comprises a clock circuit **(Thuringer, col. 3 lines 32-34, teaches that the "concepts can be realized independently of the construction of the logic (synchronous or asynchronous circuit technique)". It is inherent that if a synchronous technique is used that a clock must be present.)**,

combinatorial logic circuits **(Thuringer, Figure 2, teaches having a logic circuit that is used to mask the power consumption.)**

However, Thüringer does not specifically teach having registers.

Patterson discloses the processing unit comprises a clock circuit **(pages 134-135, Patterson teaches having a clock.)**,

combinatorial logic circuits and registers clocked by the clock circuit and connected between respective parts of the combinatorial logic circuits **(Figure 3.4, Patterson teaches a processor instruction datapath being pipelined and adding a set of registers between each pair of pipeline stages. Patterson also teaches that every pipeline stage is active on each clock cycle. Therefore, the registers must also be controlled by the clock because the values in the registers can change after each pipeline stage.)**, the pairs of processing signals comprising pairs of input and output signals of the registers **(Figure 3.4, Patterson teaches a set of registers. Each register has a set of signals coming into and going out of the register. The combination of references would include the use of registers to store/transmit data from one circuit to the next i.e. from the data processing device to the load circuit.)**,

the current drawing circuit being arranged to adjust a value of the cloaking current dependent on the activity of the registers at instants synchronized by the clock circuit **(Thüringer, Figure 3 and col. 3 lines 17-25, teaches monitoring a data processing device to generate the complementary loading current used to mask the measurable power consumption. Patterson, pages 134-135, teaches using registers to transmit data from one circuit to the next.)**

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Thüringer's invention with the teachings of Patterson. Thuringer teaches transferring data between one element to another, but is silent regarding the method of transmission. Patterson teaches using registers to transfer data from one element to another. Therefore, it would be obvious to use the registers of Patterson to transfer the data of Thuringer between the data processing device and the load circuit because adding the registers between the different combinatorial logic circuits is helpful to transfer data from one combinatorial logic circuit to the next **(Patterson, Figure 3.4, teaches the use of the pipeline registers.)**

As per claim 3, Thüringer in view of Patterson discloses an electronic circuit device according to claim 2 **[See rejection to claim 2 above]**,

organized as a pipe-line of successive parts of the combinatorial logic circuits **(Thüringer, Figure 3, teaches the use of a pipe-line. The layout of the circuit is such that the output from one set of circuits is the input into another set of circuits and this constitutes a pipe-line.)**,

each pair of successive parts coupled via a respective one or respective ones of the registers **(Patterson, Figure 3.4, teaches a processor instruction datapath being pipelined and adding a set of registers between each pair of pipeline stages. The combination of Thuringer and Patterson would result in the system of Thuringer with a register between each element.)**,

the electronic circuit device **(Thüringer, Figures 1-3, teach an electronic circuit.)**,

comprising: a plurality of activity monitor circuits **(Thüringer, Figures 2-3, teaches a set of circuits that are used to monitor the activity (logic high or low) of the incoming signals and generate a load current to mask the measurable power consumption.)**,

each coupled to receive pairs of input and output signals of the respective one or ones of the registers between a respective pair of successive parts of the combinatorial circuits **(Thuringer, Figure 2, teaches a load circuit that takes in a pair of signals and then outputs a pair of signals after processing. Thuringer, col. 1 line 45-col. 2 line 9, teaches that the load circuit monitors the power consumption of the data**

processing device. The input signal for the load circuit is the power connections i.e. Vcc (otherwise the circuit will not be functional) and also the output power consumption of the data processing device. Patterson, Figure 3.4, teaches a set of registers between each pipeline stage. Therefore, the combination would result in the elements of Thuringer having a register between them.),

and to derive a combined activity signal from the pairs of input output signals **(Thuringer, col. 1 lines 46-65, teaches the load circuit being controlled by what happens in the data processing device. Thüringer, col. 1 lines 46-52, teaches that the load circuit produces a current to be complementary to the rest of the circuit. Therefore, the load current is being added to the current that the data processing device is drawing to prevent third parties from determining the secret information by measuring the power consumed by the data processing device. The data processing device is a circuit arrangement (has multiple circuits) and the total power consumption used by the data processing device is a sum of the power used by all of the separate circuit components.)**;

a plurality of current drawing circuits connected to the power supply connections **(Thüringer, Figure 2, discloses a plurality of processing circuits such as the AND gates. It is inherent that the AND gates are connected to the power supply in order for the circuit to work.)**,

each controlled by a respective one of the activity monitor circuits to draw a cloaking current controlled by the combined activity signal derived by that respective one of the activity monitor circuits **(Thüringer, col. 1 lines 46-65, teaches the load**

circuit being controlled by at least part of the data processing device. As shown in Thüringer Figure 3, the signals that are processed by the data processing device are sent to the circuit arrangement of Figure 2 to generate the complement which is later used to control the load circuit to mask the measurable power consumption. MPEP 2144.04(V)(B) also teaches that one device can be broken down into multiple devices i.e. the load circuit of Thuringer can be broken down into the activity monitor and current drawing circuits of the Instant Application.)

As per claim 4, Thüringer in view of Patterson discloses an electronic circuit device according to claim 3 **[See rejection to claim 3 above]**,

arranged to activate the current drawing circuits in selected clock cycles when the corresponding pipe-line stages process secret information **(Thüringer, col. 1 lines 28-33 and col. 1 lines 46-65, teach using a load circuit during security-relevant operations to mask the measurable power supply. Patterson, page 134, teaches executing every stage in the pipeline during each clock cycle.)**,

14. **Claims 6, 8, and 14** are rejected under 35 U.S.C. 103(a) as being unpatentable over Thüringer in view of Kitamura et al. (US Patent 4212056) hereinafter referred to as Kitamura.

As per claims 6, 8 and 14, Thüringer discloses the current drawing circuit being arranged to adjust the value of the cloaking current so that the combination of the cloaking current and current drawn by the processing circuits substantially equals a temporal reference current pattern **(Thuringer, col. 1 lines 53-55 and col. 3 lines 25-31, teaches adjusting the loading current to mask the measurable power supply. In order to do this some reference current pattern must be present. For example, in col. 1 lines 53-55, Thuringer teaches keeping the measurable power consumption constant. Therefore, the reference current (the constant value) must be known. Also, in col. 3 lines 25-31, Thuringer teaches masking the measurable power consumption, but keeping the measurable power consumption variable and not constant.)**

However, Thuringer does not specifically disclose having a reference current pattern generator.

Kitamura discloses having a reference current pattern generator **(Kitamura, col. 6 lines 45-50, teaches comparing a detected signal to a reference current pattern to vary the pulse width in a PWM (Pulse Width Modulation) system.)**

It would have been obvious to one of ordinary skill in the art at the time the invention wad made to modify the invention of Thuringer by adding the teachings of Kitamura. Thuringer teaches masking the measurable power consumption by either keeping the output power constant or variable. If the output is constant the constant value (reference current pattern) must be known, however, Thuringer uses a different method of masking the power consumption with a variable output. It would have been obvious to replace Thuringer's method of masking the power consumption with a variable output with the use of a reference current pattern generator to generate the variable output. The combination would result in the system of Thuringer that generates a reference current pattern, compare the reference current pattern to the masked output current signal, and modify that current signal to match the reference current pattern.

Conclusion

15. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to John B. King whose telephone number is (571) 270-7310. The examiner can normally be reached on Mon. - Fri. 7:30 AM - 4:00 PM est..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/John B King/
Examiner, Art Unit 2435

/Ponnoreay Pich/
Primary Examiner, Art Unit 2435